

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ROBERT ROSS,

Plaintiff,

v.

AT&T MOBILITY, LLC,

Defendant.

Case No. 19-cv-06669-JST

**ORDER GRANTING IN PART AND
DENYING IN PART MOTION TO
DISMISS**

Re: ECF No. 16

Before the Court is Defendant AT&T Mobility, LLC's motion to dismiss. The Court will grant this motion in part and will deny it in part.

I. BACKGROUND

For the purpose of deciding the present motion to dismiss, the Court accepts as true the following factual allegations in the complaint. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001).

This action arises out of AT&T's alleged failure to protect the sensitive and confidential account information of Plaintiff Robert Ross, who is a mobile services subscriber of AT&T and a resident of San Francisco, California. *Id.* ¶¶ 1, 9. Ross contends that AT&T, a mobile services provider incorporated in Delaware, promises its customers that it will protect their privacy and will keep their personal information "safe." *Id.* ¶¶ 4, 10-11, 103. AT&T allegedly broke its promises regarding privacy and security by failing to implement sufficient data security systems and procedures, and by failing to adequately supervise its employees. *Id.* ¶¶ 4-5, 18. This failure resulted in an AT&T employee effectuating an unauthorized "SIM swap" on Ross' mobile phone, which allowed a hacker to gain unauthorized access to his financial and other accounts and steal more than \$1 million of his funds. *Id.* ¶¶ 1, 5, 44.

1 A SIM swap involves effectuating a SIM card change in a mobile phone without the
2 authorization of the owner, such that the SIM card number associated with the victim's mobile
3 account is switched from the victim's phone to a phone controlled by a hacker. *Id.* ¶¶ 18-25. This
4 re-routes the victim's mobile phone service, including any incoming data, texts, and phone calls,
5 from the victim's physical phone to a physical phone controlled by the hacker. *Id.* The hacker can
6 then use his or her control over the victim's text messages and phone calls to access and take
7 control of the victim's online accounts, such as email and banking accounts, by requesting that the
8 passwords for such accounts be reset and then using the two-factor authentication process
9 associated with such online accounts to change the password. *Id.* A SIM swap cannot take place
10 unless the mobile services carrier, through one of its employees, switches the SIM card from the
11 victim's phone to the hacker's phone. *Id.* ¶ 26.

12 Ross purchased a mobile phone services plan from AT&T in San Francisco, California, in
13 2007 for his personal use, and he has been a paying AT&T mobile services subscriber at all
14 relevant times. *Id.* ¶ 9. AT&T's "privacy commitments," which "apply to everyone who has a
15 relationship with AT&T," state that AT&T will "protect" users' privacy and will "keep [their]
16 personal information safe." *Id.* ¶ 102. These statements further provide that AT&T uses
17 "encryption and other security safeguards to protect customer data" and that it will "not sell
18 [customers'] personal information to anyone, for any purpose." *Id.* Ross alleges that these
19 representations "created an expectation" that his account and associated data would be safe and
20 secure, that AT&T employees would not access his account without authorization, and that his
21 data would be protected from unauthorized disclosure to third parties. *Id.* ¶ 103.

22 On October, 26, 2018, Ross began to receive notifications that someone was attempting to
23 withdraw money from his financial accounts, and soon after, he lost service on his mobile phone.
24 *Id.* ¶¶ 29-32. Ross took his phone to an Apple store, where he was connected to AT&T Customer
25 Support. *Id.* While on that call, an AT&T representative told him that another AT&T
26 representative had performed a SIM swap on his phone earlier that day. *Id.* The AT&T
27 representative then replaced the SIM card on his phone and restored his access to his AT&T
28 service. *Id.*

1 Later that day, Ross called AT&T customer service again, and an AT&T representative
2 identified as Ryan S. told him that the unauthorized SIM swap that had taken place earlier that day
3 had been performed by an AT&T representative named Cristelo V. in violation of AT&T's
4 policies. *Id.* ¶¶ 33-34. The unauthorized SIM swap involved customer owned and maintained
5 equipment ("COAM"), namely a mobile phone that was not provided by AT&T. *Id.* Ryan S.
6 explained that AT&T policies prohibit AT&T employees from performing a SIM swap on a
7 COAM phone pursuant to a request received by phone. *Id.*

8 During the unauthorized SIM swap of October 26, 2018, an AT&T representative accessed
9 Ross' AT&T mobile services account without authorization and was able to view and access
10 Ross' customer proprietary network information ("CPNI"), which includes information about the
11 configuration, type, and use of his subscribed AT&T services, as well as his personal information,
12 his SIM card details, and his billing information. *Id.* ¶ 53. The representative then transferred
13 control over Ross' AT&T mobile number from Ross' phone to a phone controlled by hackers by
14 performing an unauthorized SIM swap. *Id.* ¶¶ 17, 19, 37-40, 105. The hackers then immediately
15 utilized their control over Ross' mobile number to access his personal and financial accounts. *Id.*
16 ¶ 17. The hackers transferred more than \$1 million out of Ross' financial accounts. *Id.* ¶¶ 38-39.
17 The hackers also used their control over Ross' phone number to access, change the passwords, and
18 take control of several of his online accounts, including Authy, Google, Yahoo!, and Dropbox. *Id.*
19 ¶ 40. Ross had stored sensitive documents and information in these accounts, such as copies of
20 passports and birth certificates. *Id.* ¶ 45.

21 Criminal investigations revealed that a hacker named Nicholas Truglia was involved in the
22 October 26, 2018, SIM swap. *Id.* ¶ 41. These investigations also revealed that 11 unique phone
23 numbers had been SIM-swapped using Truglia's phone between October 5, 2018, and October 26,
24 2018, before the SIM swap on Ross' phone took place. *Id.* ¶ 41. Ross alleges that if AT&T had
25 conducted even the "most basic" check before authorizing SIM swaps, it would have discovered
26 that Truglia's phone had been used in the past to conduct other unauthorized SIM swaps. *Id.* ¶ 41.

27 Ross alleges that, before the SIM swap of October 26, 2018, occurred, AT&T knew or
28 should have known that its customers were at risk of unauthorized SIM swaps in light of orders

1 and publications issued by the Federal Communications Commission (“FCC”) and the United
 2 States Fair Trade Commission (“FTC”), as well as an article published online by AT&T’s Vice
 3 President of Security Platforms regarding the risk of SIM swaps. *Id.* ¶¶ 74-78. Ross also avers
 4 that AT&T was aware or should have been aware prior to the SIM swap of October 26, 2018, that
 5 there was a significant risk that its own employees would disclose, misuse, or sell customer data
 6 without authorization because videos posted online show AT&T employees discussing and
 7 analyzing these risks, including in the context of SIM swapping, and because AT&T was fined by
 8 the FCC in 2015 on the ground that AT&T employees accessed and sold the data of thousands of
 9 AT&T customers to third parties *Id.* ¶¶ 84-94.

10 Ross asserts seven claims against AT&T: (1) a claim for violations of the Federal
 11 Communications Act (“FCA”), 47 U.S.C. § 201, *et seq.*; (2) a claim for violations of California’s
 12 Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code § 17200, *et seq.*; (3) a claim for
 13 violations of the “California Constitutional Right to Privacy”; (4) a claim for negligence; (5) a
 14 claim for negligent supervision; (6) a claim for violations of the California Consumer Legal
 15 Remedies Act (“CLRA”), Cal. Civ. Code § 1750, *et seq.*; and (7) a claim for violations of the
 16 Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030.

17 **II. REQUEST FOR JUDICIAL NOTICE**

18 After the briefing on the present motion to dismiss was completed, AT&T filed a request
 19 for judicial notice of a complaint that Ross filed in a separate action captioned *Robert Ross v.*
 20 *Nicholas Truglia*, Case No. 19CV353754, in Santa Clara Superior Court. ECF No. 24; *see also*
 21 ECF No. 24-1 (state court complaint). Ross does not oppose this request.

22 “The court may judicially notice a fact that is not subject to reasonable dispute because it:
 23 (1) is generally known within the trial court’s territorial jurisdiction; or (2) can be accurately and
 24 readily determined from sources whose accuracy cannot reasonably be questioned.” Fed. R. Evid.
 25 201(b). The Court “must take judicial notice if a party requests it and the court is supplied with
 26 the necessary information.” Fed. R. Evid. 201(c)(2).

27 Because courts routinely take judicial notice of filings in other courts, the Court will grant
 28 AT&T’s request and will take judicial notice of the fact that the state-court complaint was filed.

1 *See, e.g., Harris v. County of Orange*, 682 F.3d 1126, 1132 (9th Cir. 2012) (“[Courts] may take
2 judicial notice of undisputed matters of public record, including documents on file in federal or
3 state courts.”).

4 AT&T also requests that the Court take judicial notice of the contents of the state-court
5 complaint for the purpose of resolving the present motion to dismiss. The basis for this request is
6 that Ross’ allegations in this case are inconsistent with his allegations in the state-court action.
7 According to AT&T, Ross alleges in the state-court action that “Nicholas Truglia was responsible
8 for that SIM swap,” and that “it was the bad actors (Mr. Truglia and company) that were the cause
9 of Mr. Ross’s loss, not AT&T.” ECF No. 24 at 2-3. AT&T further argues that the allegations in
10 the state-court complaint “do not allege that AT&T is part of the criminal enterprise responsible
11 for the theft.” *Id.* at 3. Based on this purported inconsistency, AT&T argues that Ross’
12 allegations in this action are not entitled to a presumption of truth.

13 Contrary to AT&T’s argument, the allegations in the state-court action are not inconsistent
14 with the allegations in the complaint in this action. As he does here, Ross alleges in the state-court
15 action that AT&T employees were involved in the SIM swap. *See, e.g.,* ECF No. 24-1 ¶¶ 14, 21.
16 The degree of AT&T’s culpability in connection with the hacking at issue is a disputed fact in this
17 action. For these reasons, the Court will not consider the contents of the state-court complaint for
18 the purpose of resolving the present motion to dismiss. *See Lee v. City of Los Angeles*, 250 F.3d
19 668, 690 (9th Cir. 2001) (holding that the district court erred by taking judicial notice of disputed
20 facts stated in public records and by failing to accept the complaint’s allegations as true and
21 drawing all inferences in the plaintiff’s favor).

22 **III. JURISDICTION**

23 The Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1332.

24 **IV. LEGAL STANDARD**

25 A pleading must contain a “short and plain statement of the claim showing that the pleader
26 is entitled to relief.” Fed. R. Civ. P. 8(a)(2). A motion to dismiss under Federal Rule of Civil
27 Procedure 12(b)(6) tests the legal sufficiency of the claims in the complaint. “To survive a motion
28 to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to

1 relief that is plausible on its face. A claim has facial plausibility when the plaintiff pleads factual
 2 content that allows the court to draw the reasonable inference that the defendant is liable for the
 3 misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation and internal quotation
 4 marks omitted). “Threadbare recitals of the elements of a cause of action, supported by mere
 5 conclusory statements, do not suffice.” *Id.* When dismissing a complaint, the court must grant
 6 leave to amend unless it is clear that the complaint’s deficiencies cannot be cured by amendment.
 7 *Lucas v. Dep’t of Corrections*, 66 F.3d 245, 248 (9th Cir. 1995).

8 Federal Rule of Civil Procedure 9(b) provides that in “alleging fraud or mistake, a party
 9 must state with particularity the circumstances constituting fraud or mistake.” Fed. R. Civ. P.
 10 9(b). “It is well-settled that the Federal Rules of Civil Procedure apply in federal court,
 11 ‘irrespective of the source of the subject matter jurisdiction, and irrespective of whether the
 12 substantive law at issue is state or federal.’” *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th
 13 Cir. 2009) (citation omitted). To satisfy Rule 9(b), the allegations regarding fraud must be
 14 “specific enough to give defendants notice of the particular misconduct which is alleged to
 15 constitute the fraud charged so that they can defend against the charge and not just deny that they
 16 have done anything wrong.” *Semegen v. Weidner*, 780 F.2d 727, 731 (9th Cir. 1985). “Averments
 17 of fraud must be accompanied by the who, what, when, where, and how of the misconduct
 18 charged.” *Kearns*, 567 F.3d at 1124 (internal citation and quotation marks omitted).

19 **V. DISCUSSION**

20 AT&T moves to dismiss every claim in the operative complaint on the ground that Ross
 21 has failed to plausibly plead proximate cause with respect to each claim. ECF No. 16 at 9. AT&T
 22 further contends that there are additional grounds that warrant dismissing certain of Ross’ claims,
 23 namely that (1) the claim for violations of the right to privacy under the California Constitution
 24 fails because Ross does not allege facts showing that he had a reasonable expectation of privacy or
 25 that AT&T’s conduct was an egregious breach of social norms; (2) the negligence claims are
 26 barred as a matter of law by the economic loss doctrine; (3) the CLRA claim fails because Ross
 27 does not plead that Ross read AT&T’s privacy policy before entering into a mobile services
 28 contract with AT&T or that any misrepresentation by AT&T occurred before he contracted with

AT&T; and (4) the claim for violations of the CFAA must be dismissed because Ross does not allege facts showing that he suffered a recoverable loss. *Id.* AT&T also moves to dismiss Ross' request for punitive damages on the grounds that Ross has not pleaded any involvement by an "officer, director or managing agent" of AT&T in any challenged conduct and has not pleaded the requisite malice, fraud, or oppression.

A. Proximate Cause

AT&T argues that *all* of Ross' claims must be dismissed because Ross has not alleged that AT&T's actions were the proximate cause "under California case law" of the theft of Ross' funds. *See* ECF No. 16 at 12-14. AT&T argues that Ross must, but cannot, allege facts plausibly showing that AT&T's conduct was the proximate cause of the theft of Ross' funds, because the theft was the result of "the independent, intervening criminal acts of others as well as perhaps his own actions and inactions." *Id.*

The Court concludes that AT&T has not shown that California's proximate cause standard is relevant to the determination of whether Ross' federal statutory claims, namely those under the FCA and CFAA, are sufficiently pleaded. AT&T argues that all of Ross' claims, including the ones under the FCA and the CFAA, should be dismissed because Ross has failed to plead facts to establish proximate cause "under California case law." *See id.* at 14 ("These holes in Mr. Ross's conclusory chain of causation defeat proximate cause as a matter of law under California case law."). But AT&T has not cited any authority showing that it would be appropriate to inject California's proximate cause standard into the analysis of claims that arise out of federal statutes.

In a footnote, AT&T cites *Bank of America Corp. v. City of Miami, Florida.*, 137 S. Ct. 1296, 1305 (2017) for the proposition that proximate cause is a required element of the federal statutory claims at issue here. ECF No. 22 at 7 n.1. But *Bank of America* does not show that proximate cause is an element of a claim under the FCA or the CFAA; nor does it answer the question of what standard of proximate cause would apply to these claims if proximate cause were an element. In *Bank of America*, the Supreme Court reaffirmed the principle stated in prior cases that, in "cases of loss," courts presume that recoverable injuries are limited to those proximately caused by the violation of the statute in question. *Id.* (citation omitted). The Supreme Court also

reiterated the principle that the “[p]roximate-cause analysis is controlled by the *nature* of the statutory cause of action. The question it presents is whether the harm alleged has a sufficiently close connection to the conduct the statute prohibits.” *Id.* (citation and internal quotation marks omitted) (emphasis added). Applying these principles to the Federal Housing Act (“FHA”) claims in that case, the Supreme Court held that a plaintiff suing under the FHA must show proximate cause because “a claim for damages under the FHA” is “akin to a tort action,” and that, based on the nature of claims under the FHA, showing proximate cause in the context of the FHA requires, based on federal common law, “some direct relationship between the injury asserted and the injurious conduct alleged.” *Id.* at 1306 (citation and internal quotation marks omitted). The Supreme Court, however, declined to “draw the precise boundaries of proximate cause under the FHA,” and remanded the case so that the lower courts could do so in the first instance. *Id.*

Here, AT&T points to no authority showing that claims under the FCA and CFAA are akin to tort actions such that a plaintiff asserting such claims is required to plead proximate cause. Further, even if pleading proximate cause were required for these claims, AT&T has pointed to no authority showing *which* standard of proximate cause would apply based on the specific “nature” of each claim.¹ Based on *Bank of America*, if any proximate cause standard would apply to these federal statutory claims, it would be one based on federal common law, and not California law. *See id.* at 1306. In light of the foregoing, the Court concludes that AT&T has not shown that Ross’ claims under the FCA and the CFAA are subject to dismissal for failure to allege facts consistent with California’s proximate cause standard.²

The Court reaches the same conclusion with respect to Ross’ California statutory claims, namely those for violations of the right to privacy under the California Constitution, the UCL, and

¹ AT&T cites *Amarillo v. Dobson Cellular*, 58 F.3d 635 (5th Cir. 1995) for the proposition that the FCA requires a showing of proximate cause. ECF No. 22 at 7 n.1. In that case, the Fifth Circuit noted in a footnote that the jury was instructed on proximate cause in connection with a claim under the FCA. That statement was dictum. Nothing in *Amarillo* establishes that a plaintiff asserting an FCA claim must plead facts to show proximate cause. Nor does it establish which standard of proximate cause would apply to an FCA claim if pleading proximate cause were required.

² Because AT&T has not advanced any other basis for dismissing Ross’ claim under the FCA, that claim survives AT&T’s motion.

the CLRA. The authorities that AT&T cites for the proposition that allegations regarding proximate cause are required for these claims are inapposite, because they address negligence claims, which arise out of the common law, or they address the standard for establishing causation in the context of an Article III standing challenge.³ See ECF No. 16 at 15. None of the authorities that AT&T cites shows that proximate cause is an element of a claim for violations of the right to privacy under the California Constitution, the UCL⁴, or the CLRA. Accordingly, the Court concludes that AT&T has not shown that Ross' California statutory claims are subject to dismissal for failure to allege facts consistent with California's proximate cause standard.

The Court addresses AT&T's argument that Ross' negligence claims are subject to dismissal for failure to plead facts consistent with California's proximate cause standard in Section V.C. of this order.

B. Right to Privacy Under the California Constitution

"Article I, section 1 of the California Constitution declares privacy an inalienable right of the people of California." *Leonel v. Am. Airlines, Inc.*, 400 F.3d 702, 711 (9th Cir. 2005), *opinion amended on denial of reh'g*, No. 03-15890, 2005 WL 976985 (9th Cir. Apr. 28, 2005) (citing Cal. Const. Art. I, § 1). "The right, in many respects broader than its federal constitutional counterpart, protects individuals from the invasion of their privacy not only by state actors but also by private parties." *Id.* (citing *Am. Acad. of Pediatrics v. Lungren*, 16 Cal. 4th 307 (1997)).

To state a claim for a violation of California's constitutional right to privacy, a plaintiff must show that he or she (1) possesses a legally protected privacy interest, (2) maintains a reasonable expectation of privacy, and (3) the intrusion is "so serious . . . as to constitute an egregious breach of the social norms" such that the breach is "highly offensive." *In re Facebook, Inc. Internet Tracking Litig.*, ___F.3d___, No. 17-17486, 2020 WL 1807978, at *7 (9th Cir. Apr. 9, 2020) (citing *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1 (1994)). "These elements do not constitute a categorical test, but rather serve as threshold components of a valid claim to be used to

³ AT&T has not asserted an Article III standing challenge in its motion.

⁴ AT&T has not advanced any other basis for dismissing Ross' claim under the UCL. That claim, therefore, survives AT&T's motion.

‘weed out claims that involve so insignificant or de minimis an intrusion on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant.’” *Id.* (quoting *Loder v. City of Glendale*, 14 Cal. 4th 846 (1997)). If the plaintiff meets these three elements, the court at a later stage of the litigation weighs the privacy interest against other competing or countervailing interests in a “balancing test.” *Pioneer Elecs. (USA), Inc. v. Superior Court*, 40 Cal. 4th 360, 371 (2007).

AT&T argues that Ross’ claim for violations of the right to privacy under the California Constitution should be dismissed because (1) Ross did not plead facts showing that he had a reasonable expectation of privacy; and (2) Ross did not plead facts showing a serious invasion of a protected privacy interest. The Court addresses each of these arguments in turn.

1. Reasonable Expectation of Privacy

AT&T alleges that Ross failed to plead with specificity the information that AT&T allegedly accessed or disclosed without his authorization, and for that reason, he fails to plead that had a reasonable expectation of privacy.

A reasonable expectation of privacy “is an objective entitlement founded on broadly based and widely accepted community norms.” *Hill*, 7 Cal. 4th at 37. To determine whether the plaintiff has a reasonable expectation of privacy, “courts consider a variety of factors, including the customs, practices, and circumstances surrounding a defendant’s particular activities.” *In re Facebook*, 2020 WL 1807978 at *7 (citing *Hill*, 7 Cal. 4th at 36). “[P]rotectable privacy interests generally fall into two categories: ‘informational privacy,’ protecting the dissemination and misuse of sensitive and confidential information, and ‘autonomy privacy,’ preventing interference with one’s personal activities and decisions.” *Pioneer Elecs.*, 40 Cal. 4th at 372. “The existence of a reasonable expectation of privacy, given the circumstances of each case, is a mixed question of law and fact.” *In re Facebook*, 2020 WL 1807978 at *7 (citing *Hill*, 7 Cal. 4th at 40). “Whether a party has a reasonable expectation of privacy is a context-specific inquiry that should not be adjudicated as a matter of law unless the undisputed material facts show no reasonable expectation of privacy.” *Leonel*, 400 F.3d at 712 (citation and internal quotation marks omitted).

Here, Ross alleges that AT&T violated his right to privacy under the California

1 Constitution by accessing and divulging, without authorization, his CPNI, which includes
2 information about the configuration, type, and use of his subscribed AT&T services, as well as his
3 personal information, his SIM card details, and his billing information. ECF No. 1 ¶ 53.

4 The relevant question is whether, in light of the customs, practices, and circumstances
5 surrounding AT&T's provision of mobile services, an AT&T customer would reasonably expect
6 that AT&T would safeguard against unauthorized access and disclosure a customer's CPNI and
7 other AT&T account information.

8 The Court concludes that Ross has plausibly alleged that an AT&T customer would
9 reasonably have expected AT&T not to access or divulge his or her CPNI without authorization in
10 light of the legal protections to which that information is subject. "CPNI is information about a
11 telephone customer's use of the telephone network, such as the number of lines ordered, service
12 location, type and class of services purchased, usage levels, and calling patterns." *People of State*
13 *of Cal. v. FCC*, 39 F.3d 919, 930 (9th Cir. 1994); *see also* 47 U.S.C. § 222(h)(1) (defining CPNI
14 as "(A) information that relates to the quantity, technical configuration, type, destination, location,
15 and amount of use of a telecommunications service subscribed to by any customer of a
16 telecommunications carrier, and that is made available to the carrier by the customer solely by
17 virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to
18 telephone exchange service or telephone toll service received by a customer of a carrier").

19 Because, as Ross alleges, CPNI can divulge a person's usage levels and calling information, the
20 FCA prohibits a telecommunications carrier from disclosing CPNI without authorization. *See* 47
21 U.S.C. § 222(c). In light of the FCA's protection of CPNI, courts have recognized that
22 telecommunications customers have a privacy interest in CPNI. *See, e.g., People of State of Cal.*,
23 39 F.3d at 930 (noting that customers "have proprietary and privacy interests in their CPNI"); *ICG*
24 *Commc'ns, Inc. v. Allegiance Telecom*, 211 F.R.D. 610, 612-15 (N.D. Cal. 2002) (noting that 47
25 U.S.C. § 222 "was principally intended to protect consumer's privacy interests" and ordering that
26 disclosure of CPNI requested in discovery be limited to attorneys' eyes only in light of the need to
27 protect such privacy interests); *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1236 (10th Cir. 1999)
28 ("[T]he specific and dominant purpose of § 222 is the protection of customer privacy.").

1 The Court further concludes that Ross has plausibly alleged that an AT&T customer would
2 reasonably have expected AT&T not to access or divulge his or her AT&T account information,
3 other than his or her CPNI, without authorization in light of AT&T's promises and statements that
4 it will protect customers' privacy and will keep their personal information "safe." ECF No. 1 ¶¶ 4,
5 10-11, 103.

6 *In re Facebook* is instructive as to why this is so. 2020 WL 1807978 at *1. There, the
7 Ninth Circuit considered whether the plaintiffs had adequately alleged claims that Facebook is
8 liable, in relevant part, for violations of their privacy rights under California law when it tracked,
9 for the purpose of selling that information to third parties, their browsing histories after they had
10 logged out of the Facebook application. *Id.* at *1. The Ninth Circuit concluded, based on
11 Facebook's statements to users, including its data use policies, that a user could have reasonably
12 assumed that his or her logged-out user data would not be collected and divulged without consent.
13 *Id.* at *7-8. Accordingly, the Ninth Circuit held that the plaintiffs had adequately alleged a
14 reasonable expectation of privacy with respect to their logged-out browsing histories. *Id.*

15 Notably, the Ninth Circuit rejected Facebook's argument that, to show a reasonable
16 expectation of privacy, the plaintiffs would "need to identify specific, sensitive information that
17 Facebook collected, and that their more general allegation that Facebook acquired an enormous
18 amount of individualized data is insufficient." *Id.* at *8 (internal quotation marks omitted). The
19 Ninth Circuit reasoned that the relevant question "is not necessarily whether Plaintiffs maintained
20 a reasonable expectation of privacy in the information in and of itself. Rather, [courts] must
21 examine whether the data itself is sensitive and whether the manner it was collected—after users
22 had logged out—violates social norms." *Id.* The Ninth Circuit concluded that, in light of the
23 "sensitivity" of the data, which revealed a person's internet activity with such specificity that
24 Facebook and others would be able to determine a user's personal interests, searches, and habits
25 on third-party websites, there were "material questions of fact as to whether a reasonable
26 individual would find the information collected" to be "sensitive and confidential." *Id.* at *9-10.
27 For that reason, the Ninth Circuit held that it could not conclude, at the pleading stage, that the
28 plaintiffs "have no reasonable expectation of privacy." *Id.* at *9.

As in *In re Facebook*, the Court here cannot conclude at the pleading stage that Ross had no reasonable expectation of privacy in the information that AT&T accessed and divulged by effectuating the unauthorized SIM swap. The SIM swap allegedly enabled the hacker to intercept Ross' phone calls and text messages,⁵ and to access any information that AT&T would have had about Ross to the extent that the hacker could use his control over Ross' telephone number to access that information. The "sensitivity" of the information at issue here is very high—and arguably higher than the information at issue in *In re Facebook*, which revealed a person's browsing activity on third-party websites—because the information here was used by the hacker to essentially impersonate Ross and intercept *the contents* of his text messages and gain access to *the contents* of his email account, financial accounts, and other accounts, among other information. See *SCC Acquisitions, Inc. v. Superior Court*, 243 Cal. App. 4th 741, 754 (2015) ("The right of privacy protects against the unwarranted, compelled disclosure of private or personal information and extends to one's confidential financial affairs as well as to the details of one's personal life.") (citation and internal quotation marks omitted). AT&T does not dispute that the contents of a person's mobile communications and email and other accounts are subject to a reasonable expectation of privacy. See ECF No. 22 at 13 (admitting that "[e]mail, Internet, and phone users" have a reasonable expectation of privacy in the "underlying contents of communication").

AT&T points to non-binding opinions⁶ that pre-date *In re Facebook* in which the courts dismissed claims for violations of the right to privacy under the California Constitution on the ground that the plaintiff did not allege, with a high degree of specificity, the exact information that was accessed or divulged by the defendant without authorization. ECF No. 16 at 19. AT&T argues, based on these non-binding opinions, that Ross has not sufficiently alleged a reasonable

⁵ AT&T argues that the interception of Ross' mobile phone account through the SIM swap revealed "nothing about the content of his communications." ECF No. 22 at 13. But Ross alleges that a SIM swap results in the hackers' interception of a user's phone calls and messages because the SIM swap allows the hackers to gain control of the user's AT&T service. The Court must construe Ross' allegations regarding the effects of the alleged SIM swap as true for the purpose of resolving the present motion.

⁶ See, e.g., *In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016 (N.D. Cal. 2014); *Zbitnoff v. Nationstar Mortg., LLC*, 2014 WL 1101161, at *4 (N.D. Cal. Mar. 18, 2014); *Albin v. Trustmark Ins. Co.*, 2013 WL 12191722, at *10 (C.D. Cal. Nov. 25, 2013).

1 expectation of privacy because he has not alleged, with a high degree of detail, the specific
 2 information that AT&T allegedly accessed or divulged. *Id.* But, in light of *In re Facebook*, 2020
 3 WL 1807978 at *1, it is not necessary for Ross to identify the “specific, sensitive information”
 4 that AT&T accessed or divulged without his authorization, because Ross has adequately alleged,
 5 as discussed above, that the type of information implicated in the unauthorized SIM swap is
 6 sensitive.

7 Accordingly, in light of the foregoing, AT&T has not shown that Ross’ claim is subject to
 8 dismissal for failure to allege a reasonable expectation of privacy.

9 **2. Serious Breach of Social Norms**

10 “Actionable invasions of privacy must be sufficiently serious in their nature, scope, and
 11 actual or potential impact to constitute an egregious breach of the social norms underlying the
 12 privacy right.” *Hill*, 7 Cal. 4th at 37. “Whether a defendant’s conduct constitutes a serious
 13 invasion of plaintiff’s privacy is a mixed question of law and fact.” *Id.* at 40. “The ultimate
 14 question of whether [a defendant’s] practices could highly offend a reasonable individual is an
 15 issue that cannot be resolved at the pleading stage.” *In re Facebook*, 2020 WL 1807978 at *11.

16 The Court concludes that Ross has adequately alleged that the manner in which his CPNI
 17 and other AT&T account information was accessed and divulged without authorization, namely
 18 through an unauthorized SIM swap performed by an AT&T employee, violates social norms in
 19 light of the expectations created by AT&T’s statements regarding the privacy and security of the
 20 information and AT&T’s legal obligations to protect its customers’ CPNI.

21 AT&T argues that Ross has failed to plead facts showing an egregious invasion of a
 22 protected privacy interest because he alleges, “at most, negligent conduct leading to an increased
 23 risk that hackers could access his personal cryptocurrency accounts,” which is not actionable.
 24 ECF No. 16 at 18.

25 This argument is unavailing. First, in addition to alleging that AT&T was negligent for
 26 failing to implement adequate security measures and for failing to adequately supervise its
 27 employees, Ross alleges *intentional* conduct by AT&T and its employees. He alleges that
 28 AT&T’s employees intentionally transferred his SIM card and AT&T account information to

hackers. *See, e.g.*, ECF No. 1 ¶ 197 (“AT&T employees, in the scope of their employment, intentionally accessed Mr. Ross’ mobile device, and assisted others in accessing his mobile device, without Mr. Ross’ authorization, in order to assist hackers in their theft of Mr. Ross.”). No case cited by AT&T addresses a similar factual scenario. Ross also alleges that AT&T intentionally misled him and other AT&T customers about its security practices, which it knew to be deficient, in order to maintain their business. *See, e.g., id.* ¶ 122 (“AT&T intentionally misled Mr. Ross regarding its data security practices in order to maintain his business, make money from his account, and evade prosecution for its unlawful acts.”); *id.* ¶ 135. This conduct amounts to more than mere negligence.

The Court concludes that Ross’ claim is not subject to dismissal for failure to plead a serious breach of social norms.

C. Negligence and Negligent Supervision

Ross asserts two tort claims against AT&T. The first is a claim for negligence and the second is a claim for negligent supervision.

“In order to establish a claim for negligence under California law, [the plaintiff] must show: (1) a legal duty to use due care; (2) a breach of that duty; and (3) that the breach was the proximate or legal cause of the injury.” *Ting v. United States*, 927 F.2d 1504, 1513 (9th Cir. 1991) (citation omitted). “Generally, whether a defendant was negligent constitutes a question of fact for the jury.” *Federico v. Superior Court (Jenry G.)*, 59 Cal. App. 4th 1207, 1214 (1997), *as modified on denial of reh’g* (Dec. 8, 1997).

“An employer may be liable to a third person for the employer’s negligence in hiring or retaining an employee who is incompetent or unfit. Negligence liability will be imposed upon the employer if it knew or should have known that hiring the employee created a particular risk or hazard and that particular harm materializes.” *Delfino v. Agilent Techs., Inc.*, 145 Cal. App. 4th 790, 815 (2006) (internal citations and quotation marks omitted). “Liability for negligent supervision and/or retention of an employee is one of direct liability for negligence, not vicarious liability.” *Id.* (citation omitted).

Here, Ross’ negligence claim is predicated on allegations that AT&T had a duty to

1 safeguard and protect Ross' CPNI and AT&T account information from unauthorized access and
 2 disclosure, which AT&T breached by failing to implement adequate security practices, failing to
 3 disclose that its security practices were inadequate, failing to detect unauthorized access to his
 4 CPNI and account information in a timely manner, and failing to supervise its employees to
 5 prevent them from accessing his CPNI and account information without authorization. ECF No. 1
 6 ¶¶ 154-69. Ross alleges that the duty that AT&T breached was based on AT&T's legal
 7 obligations under the FCA and related rules and regulations, AT&T's privacy policy, and the
 8 special relationship between Ross and AT&T that arose by virtue of AT&T's status as Ross'
 9 mobile services carrier. *Id.* ¶¶ 156-60. Ross further avers that AT&T's negligence caused Ross
 10 financial losses and severe emotional distress. *Id.* ¶¶ 167-69.

11 Ross' claim for negligent supervision is based on allegations that AT&T failed to
 12 sufficiently supervise its employees, which resulted in an AT&T employee conducting an
 13 unauthorized SIM swap on his phone. ECF No. 1 ¶¶ 170-82. Ross alleges that AT&T's
 14 insufficient oversight over its employees is evident from the fact that the SIM swap performed on
 15 his phone without his authorization was in violation of AT&T's own policies. *Id.* ¶¶ 173-74.
 16 Ross alleges that AT&T was aware or should have been aware of the risk of unauthorized SIM
 17 swaps because the hacker's phone had been used in multiple unauthorized SIM swaps before the
 18 unauthorized SIM swap on his phone took place; because of orders and publications issued by the
 19 FCC and the FTC regarding that very issue; and because AT&T was fined by the FCC in 2015 on
 20 the basis that its employees accessed and sold the data of thousands of customers to third-parties
 21 without authorization. *Id.* ¶¶ 74-78, 84-94, 181-82.

22 AT&T argues that both of these negligence claims should be dismissed (1) because Ross
 23 does not allege facts showing that AT&T proximately caused his injuries; and (2) because the
 24 claims are barred by the economic loss doctrine. The Court addresses these arguments in turn.

25 1. Proximate Cause

26 Under California law, proximate cause "is that cause which, in natural and continuous
 27 sequence, unbroken by any efficient intervening cause, produced the injury [or damage
 28 complained of] and without which such result would not have occurred." *California v. Superior*

1 *Court*, 150 Cal. App. 3d 848, 857 (1984) (citation and internal quotation marks omitted)
 2 (alteration in original). “Proximate cause, like negligence is generally held to be a question of fact
 3 for the jury.” 6 W.B. Witkin, *Summary of California Law* § 1333 (Torts) (11th ed. 2018).

4 AT&T argues that Ross’ negligence claims should be dismissed because Ross has not
 5 pleaded a “sequence of events” showing that AT&T’s actions were the proximate cause of his
 6 injuries. Specifically, AT&T contends that Ross must plead facts specifically indicating *how* the
 7 hacker gained access to each of Ross’ financial and other accounts, and that it is insufficient for
 8 Ross to merely allege that gaining control over his phone “can” be used to gain access to his
 9 financial and other accounts. *Id.* AT&T further argues that Ross cannot plead such a sequence of
 10 events because his injuries were caused by the “independent, criminal acts of others as well as
 11 perhaps his own actions or inactions.” ECF No. 16 at 12.

12 *Terpin v. AT&T Mobility, LLC*, No. 218CV06975ODWKSX, 2020 WL 883221, at *3
 13 (C.D. Cal. Feb. 24, 2020), which involves claims and allegations very similar to those at issue
 14 here, shows why AT&T is incorrect. There, the plaintiff alleged that hackers gained control over
 15 his AT&T phone number through an unauthorized SIM swap that was assisted by an AT&T
 16 employee. *Id.* at *1. This allowed the hackers to gain access to his telephone calls and text
 17 messages, and as a result, the hackers were able to use his telephone number for two-factor
 18 authentication to ultimately access his financial and other accounts and steal substantial funds
 19 from the plaintiff. *Id.*

20 The court in *Terpin* concluded that the plaintiff had sufficiently alleged proximate cause
 21 (1) by alleging that an AT&T agent was bribed by a criminal gang to transfer the SIM card on the
 22 plaintiff’s phone to the hackers’ control, which allowed the hackers to intercept communications
 23 intended for the plaintiff’s phone and reset passwords to the plaintiff’s accounts through two-
 24 factor authentication; and (2) by alleging that the hackers then accessed the plaintiff’s accounts
 25 containing confidential information, and that they used this confidential information to access the
 26 plaintiff’s financial accounts and steal his funds. *Id.* at *3. The district court rejected AT&T’s
 27 argument that the plaintiff was required to plead facts indicating the specific accounts where the
 28 plaintiff kept his confidential information and how such accounts were secured and indicating

specifically how the hackers accessed his financial accounts to steal his funds. *Id.* The court concluded that the plaintiff was not required “to reconstruct the exact sequence of the hack” at the pleading stage, and that the facts described above were sufficient to plead a “natural and continuous sequence” of plausible events connecting the hackers gaining control over his phone number with the help of an AT&T employee to the theft of his funds. *Id.*

Here, like the plaintiff in *Terpin*, Ross has pleaded sufficient facts to show a natural and continuous sequence of plausible events connecting the SIM swap performed without his authorization by an AT&T employee to the theft of his funds. Ross alleges that an AT&T employee performed an unauthorized SIM swap on his phone, which allowed the hacker to intercept his calls and text messages and use two-factor authentication to change the passwords to his accounts and ultimately access his financial and other accounts to steal his funds. These allegations are sufficient to raise the reasonable inference that the SIM swap performed by the AT&T employee was the proximate cause of the theft of his funds; Ross need not “reconstruct the exact sequence of the hack” at the pleading stage or aver additional details with respect to his accounts to adequately allege proximate cause. *See Terpin*, 2020 WL 883221, at *3.

AT&T attempts to distinguish the allegations in *Terpin* from the ones here on the ground that the plaintiff in *Terpin* alleged that he notified AT&T of a prior SIM swap, which placed AT&T “on notice that his account was vulnerable months before the damages claimed in the suit were allegedly suffered.” ECF No. 22 at 10.⁷ This difference is not dispositive, given that the *Terpin* court did not rely on allegations of prior notice to find that the plaintiff in that case had adequately pleaded proximate cause. *See Terpin*, 2020 WL 883221 at *3. But, even if prior notice were relevant to the proximate cause determination, that would still not require the dismissal of Ross’ claims. Ross has alleged sufficient facts to raise the reasonable inference that AT&T should have been on notice that his account was at risk, because Ross alleges that the hacker involved in Ross’ SIM swap had requested to transfer eleven AT&T accounts to the same phone before the unauthorized SIM swap on Ross’ account, which involved that same hacker-

⁷ AT&T cites to an opinion issued in *Terpin* that addresses an earlier iteration of the complaint and that pre-dates the opinion upon which the Court relies here. *See* ECF No. 22 at 10 (citing *Terpin v. AT&T Mobility, LLC*, 399 F. Supp. 3d 1035 (C.D. Cal. 2019)).

owned phone. ECF No. 1 ¶ 109. Ross also alleges that AT&T was aware or should have been aware of the risk of SIM swaps more generally in light of orders and publications issued by the FCC and the FTC regarding that very issue, as well as the fact that AT&T was fined by the FCC in 2015 because its employees accessed and sold the data of thousands of customers to third parties without authorization. *Id.* ¶¶ 74-78, 84-94. Accordingly, the Court concludes that Ross’ negligence claims are not subject to dismissal for failure to adequately plead proximate cause.

AT&T also argues that Ross’ negligence claims fail as a matter of law because the theft of his funds was caused by the “independent” criminal acts of third parties, which are unforeseeable. ECF No. 16 at 16 (citing *Jesse v. Malcmacher*, 2016 WL 9450683, at *10 (C.D. Cal. Apr. 5, 2016) (“The illegal acts of third parties are unforeseeable as a matter of law.”)). This argument is unpersuasive.

“[T]he defense of ‘superseding cause[]’ . . . absolves [the original] tortfeasor, even though his conduct was a substantial contributing factor, when an independent event [subsequently] intervenes in the chain of causation, producing harm of a kind and degree so far beyond the risk the original tortfeasor should have foreseen that the law deems it unfair to hold him responsible.” *Chanda v. Fed. Home Loans Corp.*, 215 Cal. App. 4th 746, 755 (2013) (citation omitted) (alterations in the original). “To qualify as a superseding cause so as to relieve the defendant from liability for the plaintiff’s injuries, both the intervening act and the results of that act must not be foreseeable. Significantly, what is required to be foreseeable is the general character of the event or harm . . . not its precise nature or manner of occurrence.” *Id.* (internal citations and quotation marks omitted) (alteration in original). “Whether an intervening force is superseding or not generally presents a question of fact, but becomes a matter of law where only one reasonable conclusion may be reached.” *Id.* (citation omitted).

Here, Ross alleges that the SIM swap was facilitated by an AT&T employee, who is not an “independent” third party. *See Williams v. AT&T Mobility, LLC*, No. 5:19-CV-475-BO, 2020 WL 1492803, at *4 (E.D.N.C. Mar. 25, 2020) (denying motion to dismiss claims arising out of unauthorized SIM swap based on the argument that the plaintiff failed to plead proximate cause in part because “the criminal conduct in a SIM swap is not ‘independent,’ but is facilitated by the

wireless carrier”). Although AT&T implies that it did not have control over the employee who performed the unauthorized SIM swap on Ross’ phone, the question of AT&T’s control or supervision over its employees for the purpose of invoking the superseding-cause defense is one of fact that cannot be resolved as a matter of law at the pleading stage. Nor can the Court resolve as a matter of law at this juncture the question of whether the actions of the hacker subsequent to the SIM swap were foreseeable, as Ross has alleged sufficient facts to raise the inference that AT&T knew or should have known of the risks and potential consequences of unauthorized SIM swaps. Accordingly, the Court concludes that Ross’ negligence claims cannot be dismissed as a matter of law on the basis of the defense of superseding cause.

2. Economic Loss Doctrine

AT&T argues that Ross’ negligence claims are barred by the economic loss doctrine because they arise out of disappointed expectations in connection with AT&T’s performance of a contract between Ross and AT&T, and because they are not based on the breach of a duty that is independent of that contract. ECF No. 16 at 20-21. AT&T further argues that the “special relationship” exception to the economic loss rule does not apply to Ross’ negligence claims because Ross and AT&T are in privity, and because Ross has failed to allege facts showing that a special relationship between the parties exists.

Under the economic loss rule, economic losses suffered as a result of the negligent breach of a contract for goods or products “are not recoverable under negligence.” *S.M. Wilson & Co. v. Smith Int’l, Inc.*, 587 F.2d 1363, 1376 (9th Cir. 1978) (citing *Seely v. White Motor Co.*, 63 Cal. 2d 9, 18 (1965)). The economic loss rule “serves to limit the parties’ rights to those provided by the Uniform Commercial Code, a body of law specifically designed to deal with commercial disputes between sellers and buyers of goods.” *Id.* The purpose of the rule is to “prevent[] the law of contract and the law of tort from dissolving one into the other.” *Robinson Helicopter Co. v. Dana Corp.*, 34 Cal. 4th 979, 988 (2004) (citation omitted).

The economic loss rule does not apply, however, where the contract between the parties does not involve the sale of goods or products, because such contracts are not governed by the Uniform Commercial Code. *See* 6 B.E. Witkin, *Summary of California Law* § 1681 (Torts) (11th

ed. 2018) (“The ‘economic loss’ rule does not apply when the commercial relationship of the parties does not involve the sale of goods or products, nor the rules developed under the law merchant and the Uniform Commercial Code. In these cases, the policy concerns underlying the limitations on recovery of economic losses articulated by the court in *Seely v. White Motor Co.* are not present.”). Accordingly, “the economic loss rule does not apply when the contract alleged to be negligently performed relates to the performance of services.” *Id.* (citation omitted); *see also N. Am. Chem. Co. v. Superior Court*, 59 Cal. App. 4th 764, 770 (1997) (holding that the “so-called ‘economic loss rule’ does not bar recovery” of economic losses in a tort action that “arises from a contract for the performance of services rather than the sale of goods”).

Here, the economic loss rule would bar Ross from recovering economic damages in connection with his negligence claims only if such claims are based on allegations (1) that his economic damages were caused by the negligent breach of a contract; and (2) that contract was for the sale of goods or products. Ross’ allegations do not meet these criteria. No contract for goods or products is alleged in the complaint. The only contract alleged in the complaint is one between Ross and AT&T for the provision of mobile *services*.⁸ ECF No. 1 ¶¶ 9, 1, 2. Because of the absence of an alleged contract for goods or products, the economic loss rule does not preclude Ross from recovering economic losses in connection with his negligence claims.⁹ *See Corelogic, Inc. v. Zurich Am. Ins. Co.*, No. 15-CV-03081-RS, 2016 WL 4698902, at *5 (N.D. Cal. Sept. 8, 2016) (holding that the economic loss rule “does not apply to the instant case” because the tort claims were based on allegations that “defendants negligently performed an attendant professional service”) (emphasis added).

AT&T cites non-binding cases for the proposition that the economic loss rule bars tort claims *in their entirety* even if they are based on the breach of a contract for services. *See* ECF

⁸ This distinguishes the facts here from those in *Hammond Enterprises Inc v. ZPS Am. LLC*, No. C-12-03600(EDL), 2013 WL 5814505, at *4 (N.D. Cal. Oct. 29, 2013) (applying economic loss rule to claim based on breach of a contract for sale of machines that failed to perform according to the contract).

⁹ The economic loss rule, which only precludes the recovery of economic damages in a tort action, would in no event bar Ross’ negligence claims as a whole because Ross’ negligence claims are not limited to seeking economic damages; he also alleges to have suffered emotional distress as a result of AT&T’s conduct. *See* ECF No. 1 ¶ 168.

No. 16 at 21-22. The Court finds the reasoning in these opinions to be unpersuasive. Although the courts in those cases applied the economic loss rule in the context of contracts for services, none of them mention, and they appear not to have considered, the distinction between contracts for services and those for goods.¹⁰ Consequently, those courts failed to recognize that the negligent breach of a contract for services can give rise to *both* a tort and a breach-of-contract claim, where the former arises out of “a breach of a duty growing out of contract” and the latter arises out of the “breach of a promise set forth in the contract.” *S.M. Wilson*, 587 F.2d at 1376 (citation omitted). “A contract to perform services gives rise to a duty of care” that is independent of the express terms of the contract, “which requires that such services be performed in a competent and reasonable manner.” *N. Am. Chem.*, 59 Cal. App. 4th at 774. Accordingly, a negligent breach of a services contract can give rise to “both a breach of contract and a tort.” *Id.* (internal citations omitted); *see also Moreno v. Sanchez*, 106 Cal. App. 4th 1415, 1435 (2003) (“Under the common law the established rule is the negligent failure to exercise reasonable care and skill in undertaking to perform a service contract of this type is a tort, as well as a breach of contract.”).

AT&T also argues that Ross’ negligence claims should be dismissed because they are based on disappointed expectations arising out of Ross’ mobile services contract with AT&T, and not on the breach of any duty independent of that contract. ECF No. 16 at 21-22.

AT&T misapprehends the nature of Ross’ negligence claims. Ross’ negligence claims are *independent* of the express terms of any contract. They are based on the theory that AT&T breached a duty of care¹¹ that arose by virtue of AT&T’s legal obligations as a carrier subject to the FCA and related rules and regulations,¹² by virtue of AT&T’s role as his mobile services

¹⁰ One of the cases is unpersuasive for the additional reason that it applied Massachusetts, not California, law. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014).

¹¹ “Liability for negligent conduct may only be imposed where there is a duty of care owed by the defendant to the plaintiff or to a class of which the plaintiff is a member. . . . Such duty can arise from statute or contract, the nature of defendant’s activity, the relationship between the parties, “or even the interdependent nature of human society.” *Ott v. Alfa-Laval Agri, Inc.*, 31 Cal. App. 4th 1439, 1449 (1995) (citation omitted).

¹² Ross alleges that the FCA required AT&T to, among other things, take steps to ensure that its

1 carrier, and by virtue of AT&T's statements in its privacy policy. *Id.* ¶¶ 156-60. Thus, Ross'
2 negligence claims are based on (1) the alleged breach of legal duties, and (2) duties arising out the
3 relationship that existed between Ross and AT&T by virtue of Ross' mobile services agreement
4 with AT&T.

5 AT&T offers no basis in its motion for dismissing the negligence claims to the extent that
6 they are based on AT&T's alleged breach of its legal duties under the FCA and related rules and
7 regulations; accordingly, these claims survive AT&T's motion.

8 AT&T argues that Ross' negligence claims should be dismissed to the extent that they are
9 based on the alleged breach of a duty arising out of a "special relationship" between it and Ross.

10 Where, as here, a plaintiff brings a tort claim based on the breach of duty of care arising
11 out of a contract for services, the plaintiff may recover economic losses and any other remedies
12 available in tort if the plaintiff can show that a special relationship existed between it and the
13 defendant. *N. Am. Chem.*, 59 Cal. App. 4th at 785. In this context, the existence of a "special
14 relationship" is used to show that a "duty of care existed" between the plaintiff and defendant
15 pursuant to which the defendant can be held liable in tort. *Ott v. Alfa-Laval Agri, Inc.*, 31 Cal.
16 App. 4th 1439, 1450 (1995).

17 Courts employ the following six-part test, which is derived from *J'Aire Corp. v. Gregory*,
18 24 Cal. 3d 799, 804 (1979) and is therefore known as the "*J'Aire* test," to determine whether the
19 requisite "special relationship" exists: "(1) the extent to which the transaction was intended to
20 affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the
21 plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and
22 the injury suffered, (5) the moral blame attached to the defendant's conduct, and (6) the policy of
23 preventing future harm." *N. Am. Chem.*, 59 Cal. App. 4th at 782 (citing *J'Aire*, 24 Cal. 3d. at

24
25
26 CPNI is adequately protected by unauthorized disclosure. *See, e.g.*, ECF No. 1 ¶ 54 n.18 (citing
27 47 U.S.C. § 222(c)(1), which provides, in relevant part, that "[e]very telecommunications carrier
28 has a duty to protect the confidentiality of proprietary information of, and relating to, other
telecommunication carriers, equipment manufacturers, and customers"). Ross also alleges that
FCC rules promulgated pursuant to the FCA required AT&T to enact effective safeguards to
protect against the unauthorized disclosure of CPNI. ECF No. 1 ¶¶ 57-59.

804). “[T]hese factors essentially help identify whether there is an unusual degree of foreseeability of the particular injury the plaintiff has suffered.” *Ott*, 31 Cal. App. 4th at 1450.

AT&T argues that Ross cannot sue it in tort based on a “special relationship,” because “special relationship” tort liability is limited to circumstances where the plaintiff and the defendant are not in contractual privity. This argument is unpersuasive. Although *J’Aire* involved a plaintiff and defendant who were not in contractual privity,¹³ “[s]ubsequent cases have extended the application of *J’Aire* to cases where the parties are in contractual privity.” *N. Am. Chem.*, 59 Cal. App. 4th at 783 (collecting cases). Accordingly, for the purpose of determining whether a special relationship exists under the *J’Aire* test, “it does not matter if the plaintiff and the defendant are in privity or not.” *Id.* at 785.

AT&T also argues that, even if a “special relationship” could be invoked where the parties are in privity, Ross has not alleged facts to show that he and AT&T had a “special relationship.”

In *Terpin*, 2020 WL 883221 at *4, which, as discussed above, involves claims arising out of a SIM swap based on allegations very similar to those at issue here, the court concluded that the plaintiff had alleged sufficient facts to show that he had a “special relationship” with AT&T under the *J’Aire* test. The court found that the first factor was met because the plaintiff was required to share his personal information with AT&T as a result of the mobile services agreement he had with AT&T, and that the sharing of this information was based on the understanding that AT&T would protect that information. *Id.* The court found that the second factor was satisfied because the plaintiff sufficiently alleged that it was foreseeable that he would suffer injury if AT&T did not protect his personal information. *Id.* As to the third factor, the court found that it was met

¹³ In *J’Aire*, the plaintiff argued that the defendant owed it a duty of care because of the “special relationship” that existed between the plaintiff and the defendant by virtue of a contract to which the defendant, but not the plaintiff, was a party. 24 Cal. 3d. at 804. Based on the six-part test described above, the court concluded that the contract was intended to directly affect the plaintiff because the contract required the defendant to improve the space where the plaintiff ran its business. *Id.* The court also concluded that economic injury to the plaintiff was clearly foreseeable because the plaintiff could lose business as a result of the defendant’s failure to improve the space where plaintiff ran its business. *Id.* at 804-05. The court therefore held that the plaintiff could sue the defendant for economic damages based on a theory of negligent interference with prospective economic advantage based on the defendant’s breach of the contract, even though the plaintiff and the defendant were not in privity. *Id.*

1 because the plaintiff pleaded facts to show that the injury he suffered as a result of the SIM swap
 2 was certain. *Id.* As to the fourth factor, the court found that it was met because he suffered
 3 damages as a result of AT&T's failure to protect his SIM card. *Id.* As to the fifth factor, the court
 4 found that it was met because AT&T was aware of the risk of SIM swaps yet failed to protect its
 5 customers' accounts. *Id.* As to the sixth factor, the court found that it was met because AT&T's
 6 failure to adequately protect the plaintiff's personal information implicates the consumer data
 7 protection concerns expressed in federal statutes, including the FCA. *Id.*

8 The Court concludes that the same allegations that the court in *Terpin* found to be
 9 sufficient to plead a "special relationship" with AT&T under the *J'Aire* test have also been alleged
 10 by Ross in this case. Accordingly, the Court concludes that Ross' negligence claims are not
 11 subject to dismissal on the basis that he has failed to plead a "special relationship" with AT&T.

12 **D. CLRA**

13 The CLRA prohibits "unfair methods of competition and unfair or deceptive acts or
 14 practices undertaken by any person in a transaction intended to result or that results in the sale or
 15 lease of goods or services to any consumer." Cal. Civ. Code § 1770(a). The Act proscribes
 16 "[r]epresenting that goods or services have . . . characteristics . . . uses, benefits, or quantities
 17 which they do not have," *id.* § 1770(a)(5), and "[r]epresenting that goods or services are of a
 18 particular standard, quality, or grade," *id.* § 1770(a)(7).

19 Ross asserts a claim under the CLRA. ECF No. 1 ¶¶ 183-94. It is based on the theory that
 20 AT&T, through misrepresentations and omissions, misled its customers regarding the adequacy of
 21 its practices to protect its customers' information and privacy, and that AT&T actively concealed
 22 that its data protection practices were inadequate to protect its customers' data. *Id.*

23 AT&T argues that Ross' claim under the CLRA should be dismissed because (1) Ross did
 24 not plead reliance on any of AT&T's alleged misrepresentations or omissions; and (2) all of the
 25 alleged misrepresentations and omissions occurred after his decision to contract with AT&T.

26 Where, as here, the plaintiff brings a claim under the CLRA based on the defendant's
 27 misrepresentations or omissions, the claim sounds in fraud and must satisfy the heightened
 28 pleading requirements of Rule 9(b). *See Kearns*, 567 F.3d at 1124-27. To state a claim under the

CLRA based on a fraudulent misrepresentation theory, the plaintiff must show “actual reliance on the misrepresentation and harm.” *Sateriale v. R.J. Reynolds Tobacco Co.*, 697 F.3d 777, 794 (9th Cir. 2012) (citations and internal quotation marks omitted). Likewise, to state a claim under the CLRA for fraudulent omission, a plaintiff first must show that he or she actually relied on the omission. *Daniel v. Ford Motor Co.*, 806 F.3d 1217, 1225 (9th Cir. 2015) (“An essential element for a fraudulent omission claim is actual reliance”) (citing *Cohen v. DIRECTV, Inc.*, 178 Cal. App. 4th 966 (2009)).

Here, Ross alleges that AT&T’s privacy policy, in which AT&T promises to protect customers’ privacy and implement security safeguards, “created an expectation” that his AT&T account information would be safe and secure from unauthorized access and disclosure. ECF No. 1 ¶¶ 101-06. Ross also avers that his “willingness to contract with AT&T, and thereby entrust AT&T with his confidential and sensitive account data, was predicated on the understanding that AT&T would undertake adequate security and consent precautions.” *Id.* ¶ 161.

Ross, however, does not allege the date of the AT&T statements and omissions that underlie his CLRA claim. The date of such statements and omissions matters because, if AT&T made them after Ross decided to initially contract or renew a contract with AT&T, then that would preclude him from asserting a claim under the CLRA. The CLRA prohibits misrepresentations and omissions “intended to result or that result[] in the sale or lease of goods or services to any consumer.” Cal. Civ. Code § 1770. “Thus, it is the defendant’s *pre-sale* representations and omissions that matter under the CLRA.” *Hensley-Maclean v. Safeway, Inc.*, No. CV 11-01230 RS, 2014 WL 1364906, at *7 (N.D. Cal. Apr. 7, 2014) (collecting cases) (emphasis added). Ross states in his opposition that the statements in question were made by AT&T in 2006, prior to him entering into a contract with AT&T in 2007, but that date is not alleged in the complaint. Because Ross has not alleged facts raising the reasonable inference that the statements and omissions at issue were made by AT&T prior to Ross’ decision to initially contract, or to renew a contract, with AT&T, Ross has not adequately pleaded reliance and the Court will dismiss his CLRA claim on that basis, with leave to amend.

E. Computer Fraud and Abuse Act

“The CFAA was enacted in 1984 to enhance the government’s ability to prosecute computer crimes.” *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130-31 (9th Cir. 2009). “The act was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to access and control high technology processes vital to our everyday lives[.]” *Id.* (citation and internal quotation marks omitted). “The CFAA prohibits a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data.” *Id.* To maintain a civil action under the CFAA, the plaintiff must show (1) that he or she “suffer[ed] damage or loss by reason of [the defendant’s] violation” of the Act, and (2) that one of five enumerated circumstances in § 1030(c)(4)(a)(i)(I) through (V)¹⁴ is present. 18 U.S.C. § 1030(g).

AT&T challenges the sufficiency of Ross’ allegations only with respect to the second element of an FCAA claim under § 1030(g), which requires a showing that one of the five enumerated circumstances in § 1030(c)(4)(a)(i)(I) through (V) is present. The circumstance set forth in subpart (I) requires a plaintiff to show a “loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value.” ECF No. 21 at 23 (quoting 18 U.S.C. § 1030(c)(4)(A)(i)(I)). In his complaint, Ross states that he “spent in excess of \$5,000 investigating who accessed his mobile device and damaged information on it.” ECF No. 1 ¶ 202. AT&T argues that this allegation is conclusory because it lacks facts describing the details of Ross’ investigation or costs of any investigative steps. ECF No. 16 at 30-31.

¹⁴ The five enumerated circumstances are: “(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value; (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; [and] (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security[.]”

The Court in *NovelPoster* found allegations like those here to be sufficient to allege a loss within the meaning of 18 U.S.C. § 1030(c)(4)(A)(i)(I). There, plaintiffs alleged that they “each spent substantial time and energy ‘on their efforts to secure the restoration of NovelPoster and its data and information’ to the condition they were in ‘prior to when defendants took control of NovelPoster,’ efforts which included restoring the data and information to their prior condition, as well as responding to and conducting a damage assessment of defendants’ alleged CFAA and CDAFA violations.” *NovelPoster*, 140 F. Supp. 3d at 962 (quoting the first amended complaint in that case). AT&T complains that Ross, unlike the *NovelPoster* plaintiffs, has not alleged the approximate number of hours that he spent on his restorative efforts, and the approximate value of his own services, ECF No. 22 at 18, but the absence of this information does not impair Ross’ claim. For one thing, AT&T cites no authority imposing a requirement that a CFAA loss be pled with specificity. For another, unlike the plaintiffs in *NovelPoster*, Ross need not attribute a value to his own time, because the allegation in the complaint is that he spent money on services provided by other people.

Accordingly, the Court denies AT&T’s motion to dismiss Ross’ claim under the CFAA.

F. Punitive Damages

“In an action for the breach of an obligation not arising from contract, where it is proven by clear and convincing evidence that the defendant has been guilty of oppression, fraud, or malice, the plaintiff, in addition to the actual damages, may recover damages for the sake of example and by way of punishing the defendant.” Cal. Civ. Code § 3294(a). A corporate employer cannot be liable for punitive damages under § 3294(a) unless “an officer, director, or managing agent of the corporation” had “advance knowledge of the unfitness of the employee and employed him or her with a conscious disregard of the rights or safety of others or authorized or ratified the wrongful conduct for which the damages are awarded or was personally guilty of oppression, fraud, or malice.” Cal. Civ. Code § 3294(b). “Malice” means “conduct which is intended by the defendant to cause injury to the plaintiff or despicable conduct which is carried on by the defendant with a willful and conscious disregard of the rights or safety of others.” Cal. Civ. Code § 3294(c)(1).

AT&T moves to dismiss Ross' request for punitive damages on the basis that Ross fails to allege that any officer, director, or managing agent of AT&T knew about, committed, ratified, or authorized any of the actions about which Ross complains. ECF No. 16 at 32. AT&T also argues that Ross' allegations regarding malice, fraud, and oppression are conclusory. *Id.* at 33.

In his opposition, Ross cites *ExxonMobil Oil Corp. v. S. California Edison Co.*, No. CV1210001GHKVBKX, 2013 WL 12166214, at *3 (C.D. Cal. May 1, 2013) for the proposition that his allegations are sufficient to state a basis for punitive damages under § 3294(b) based on the theory that AT&T acted with malice at the officer, director, or managing agent level. In that case, the district court rejected the defendant's argument that the plaintiff had failed to plead that the defendant, through an officer, director, or managing agent, committed acts that were willful or in conscious disregard of the rights of the plaintiff (i.e., with malice). *Id.* The court found that the plaintiff's allegations were sufficient to plausibly plead entitlement to punitive damages under § 3294(b) because the plaintiff alleged facts showing that the defendant had previously indicated its understanding of plaintiff's critical need for a reliable supply of electricity in light of several past outages and litigations, and because the defendant made "repeated assurances of reliability" as a result. *Id.* In light of these allegations, the district court concluded that the plaintiff had plausibly alleged that subsequent power outages occurred as a result the defendant's conscious disregard, at the level of officer, director, or managing agent, of its obligations and promises regarding a reliable supply of electricity. *Id.*

Here, Ross alleges conduct similar to what the court in *ExxonMobil* found to be sufficient to state a basis for punitive damages under § 3294(b). Ross alleges that AT&T had a history of its own employees disclosing customer information without authorization, because AT&T was fined by the FCC in 2015 on the ground that AT&T employees accessed and sold the data of thousands of AT&T customers to third parties. ECF No. 1 ¶¶ 84-94. Ross also alleges that AT&T was aware of the risk of SIM swaps in light of orders and publications issued by the FCC and the FTC, as well as an article published online by AT&T's Vice President of Security Platforms regarding the risk of SIM swaps. *Id.* ¶¶ 74-78. Ross also avers that AT&T is required by the FCA and related rules and regulations to protect customers' CPNI and other sensitive information, and that

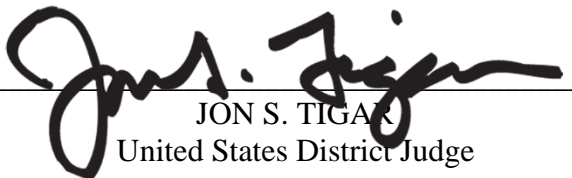
1 it has made promises, including in its privacy policy, that it would protect its customers'
 2 information. *Id.* ¶¶ 57-59, 156-60. Ross further avers that AT&T failed to implement adequate
 3 security and employee-supervision measures to protect its customers' information notwithstanding
 4 these assurances. *Id.* The Court concludes that these allegations are sufficient to raise the
 5 inference that Ross' unauthorized SIM swap occurred as a result of AT&T's willful and conscious
 6 disregard, at the level of officer, director, or managing agent, of its obligations to protect its
 7 customers' information from unauthorized disclosure pursuant to its own promises and its legal
 8 obligations under the FCA and related rules and regulations. *See ExxonMobil Oil Corp.*, 2013 WL
 9 12166214 at *3. AT&T did not address *ExxonMobil* in its reply. Accordingly, the Court will
 10 deny AT&T's motion to dismiss Ross' request for punitive damages.

11 CONCLUSION

12 For the foregoing reasons, the Court grants in part and denies in part AT&T's motion to
 13 dismiss. The motion is granted, with leave to amend, with respect to Ross' claim under the
 14 CLRA. The motion is otherwise denied. Within 21 days of the date this order is filed, Ross may
 15 file an amended complaint for the purpose of curing the deficiencies identified herein in
 16 connection with his claim under the CLRA to the extent that he can do so without contradicting
 17 the allegations in the original complaint. Ross may not assert any new claims in the amended
 18 complaint.

19 **IT IS SO ORDERED.**

20 Dated: May 14, 2020

21 
 22 JON S. TIGAR
 23 United States District Judge
 24
 25
 26
 27
 28